Federal Bridge CA Certificate Policy
Change Proposal

Change Serial Number: 2001-13

Title: Clarify applicability of system development controls to Agency CAs

Date: 05 November 2001

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), dated 14 June 2001

Change Advocate Contact Information:

Name: Mike Jenkins
Organization: DoD
Telephone number:
E-mail address: mjjenki@missi.ncsc.mil

Organization requesting change: CPWG

Change summary: Clarify the system development controls requirements to indicate their applicability to Agency CAs at the High and Medium levels of assurance, in addition to the FBCA.

Background:
The CP currently levies system development controls on the FBCA. It explicitly levies one development control on Agency CAs. The applicability of the remainder of the controls are ambiguous; while there is no explicit levy, the controls will nonetheless be considered during the policy mapping. Confusion comes from the simultaneous use of explicit and implicit requirements. The proposed text below removes the ambiguity by making the requirement explicitly binding on Agency CAs at the High and Medium levels of assurance (in addition to the FBCA).

Specific Changes:

Existing text:
Section 6.6.1, System development controls:

The System Development Controls for the FBCA are as follows:

The FBCA or Agency CA shall use software that has been designed and developed under a formal, documented development methodology.

Hardware and software procured to operate the FBCA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).

Hardware and software developed specifically for the FBCA shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.

All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the FBCA physical location.

The FBCA hardware and software shall be dedicated to performing one task: the FBCA. There shall be no other applications; hardware devices, network connections, or component software installed which are not part of the FBCA operation.

Proper care shall be taken to prevent malicious software from being loaded onto the FBCA equipment. Only applications required to perform the operation of the FBCA shall be obtained from sources authorized by local policy. RA hardware and software shall be scanned for malicious code on first use and periodically thereafter.

[final bullet not included]

Proposed revised text:

Modify sentence introduction and bullets as follows:

The System Development Controls for the FBCA and Agency CAs at the Basic Assurance level and above are as follows:

Use software that has been designed and developed under a formal, documented development methodology.

Hardware and software procured to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).

Hardware and software developed specifically for the CA shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.

All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the CA physical location.

The CA hardware and software shall be dedicated to performing one task: the FBCA. There shall be no other applications; hardware devices, network connections, or component software installed which are not part of the CA operation.

Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Only applications required to perform the operation of the CA shall be obtained from sources authorized by local policy. RA hardware and software shall be scanned for malicious code on first use and periodically thereafter.

[final bullet unchanged]

Estimated Cost:

Agencies that have purchased CA equipment from established PKI product or service vendors through normal agency procurement channels, having equipement directly drop-shipped from the vendor, or having a system built by an integrator who builds many such systems, should have already met these requirements. Extra care may need to be exercised by agencies who have procured or that will procure custom systems using components procured from resellers outside normal agency procurement channels.

Implementation Date:

This change will be implemented immediately.

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG: 05 November 2001
Date CPWG recommended approval: 05 November 2001
Date Presented to FPKI PA:
Date of approval by FPKI PA: